DEPARTMENT OF THE NAVY
NAVY RECRUITING DISTRICT, PORTLAND
7028 N.E. 79TH COURT
PORTLAND, OREGON 97218-2813

NAVCRUITDISTPORTLANDINST 5239.1D
SYSAD
26 Mar 13

NAVCRUITDIST PORTLAND INSTRUCTION 5239.1D

Subj: NAVY RECRUITING DISTRICT (NRD) PORTLAND INFORMATION SYSTEMS SECURITY (INFOSEC) PROGRAM

Ref: (a) COMNAVCRUITCOMINST 5239.1A
(b) OPNAVINST 5239.1C
(c) COMNAVCRUITCOMINST 5400.2E
(d) NAVCRUITDISTPORTLNDINST 5239.2B
(e) COMNAVCRUITCOMINST 4400.1D (Chapter 3)

Encl: (1) Spot Check Form (COMNAVCRUITCOM 4400.1C (Chapter 3))
(2) Microcomputer Standard Operating Procedures (SOP)/ Microcomputer SOP Review Acknowledgment (PTLDO 5230/3 (Rev. 3-13)
(3) Information System (IS) Security Briefing/User Briefing/User Responsibility Agreement (NAVCRUIT 5239/5 (Rev. 02-01)
(4) AIS Security Incident Report (COMNAVCRUITCOM 5239/1 (Rev. 8-2011))
(5) CNRC Custody Card for Notebook Computers (COMNAVCRUITCOM 5230/6 (Rev. 3-08)

1. Purpose. To integrate provisions of references (a) through (e) and enclosures (1) through (5) to Navy Recruiting District (NRD) Portland's Information Systems Security (INFOSEC) Program and to issue uniform policies for all information systems, equipment, networks, and processed data. Reference (a) should be reviewed in its entirety.

2. Cancellation. NAVCRUITDIST Portland Instruction 5239.1C.

3. Background. References (a) through (c) directs NRD Portland to implement and maintain an Automated Information Systems (AIS) security program to assure that adequate security is provided for all information collected, processed, transmitted, stored, and disseminated in general support systems and major applications. With technological advancements in communications has come increased danger of losing sensitive data and ultimately crippling our organization through vulnerabilities in these systems. This policy is designed to bring these vulnerabilities to a level of risk that will protect our resources without unduly impeding production. All sensitive but unclassified systems must be safeguarded so that such information is only accessed by authorized persons, is used only for its intended purpose, retains its content integrity, and is marked properly as required.

4. Scope. The Commander, Navy Recruiting Command (CNRC) is responsible for ensuring compliance with DON INFOSEC Program

identified in references (a) and (b). The procedures and principles presented in these guidelines apply to all Recruiting District military and civilian employees (including government contractors) who have access to any CNRC AIS system.

5. Policy. Organizational heads are responsible for ensuring their employees comply with this policy and use the Internet for official government business and other authorized purposes only. Individual users will be held accountable for their use and Internet access. Unless access to an external or internal function or system is specifically allowed, the function or system access is not allowed. Allowing only minimum set of accesses ensures that if users make mistakes, or if intruders succeed in masquerading as legitimate users, the scope of the potential damage is limited.

a. Spot Checks. Per reference (e), random Spot Checks will be done monthly by selecting stations or departments by using the Spot Check form(s) at enclosure (1). This is to ensure accountability has been maintained between inventories.

b. Semi-Annual Inventory. An Automated Information Systems (AIS) equipment inventory report will be issued to each station and department on a semi-annual basis. All personnel responsible will verify and update the NRD inventory. Personnel responsible for the equipment will return their inventory within five working days.

c. Microcomputer Standard Operating Procedures (SOP), enclosure (2), will be issued to all users upon check-in. This is to ensure current standard operating procedures inclusive of Automated Information System (AIS) practices and procedures are available and used by all information technology resource users.

d. CNRC Privilege User Agreement/Authorization Brief, enclosure (3), will be issued to all users upon check-in. Personnel requesting access to the CNRC LAN/WAN will require training prior to access and will require a logon and password. The Information System Security Officer (ISSO) will submit in writing the established NAVCRUIT 5239/5, and any specific requirements for access, to the SYSAD prior to access. The form will be retained for the duration that an individual is attached to the command.

e. Information System Security Incidents. All incidents that influence the security and integrity of command computer systems will be reported immediately to the local ISSO. The ISSO will then investigate each incident thoroughly and recommend appropriate corrective action to prevent recurrence to the Commanding Officer. The ISSO will report all security violations and/or incidents to the

CNRC Information System Security Manager (ISSM), utilizing the NAVCRUIT 5239/1, AIS Security Incident Report, at enclosure (4).

6. Action. All Headquarters staff and all Recruiting field activities will adhere to the policies and procedures contained in this instruction and reference (a).

7. Forms

a. PTLDO 5230/3 (Rev. 9-02), Microcomputer Standard Operating Procedures (SOPs) Review Acknowledgement, can be obtained from the Forms Manager or the Systems Administrator.

b. NAVCRUIT 5239/1 (Rev. 4-00), AIS Security Incident Report; NAVCRUIT 5239/5 (Rev. 02-01), Briefing/User Responsibility Agreement; and NAVCRUIT 5230/6 (Rev. 3-96), CNRC Custody Card for Notebook Computers is available electronically via the CNRC Quarterdeck web site at https//rq.cnrc.navy.mil.

R. M. CANDILORO

Distribution:
NAVCRUITDISTPORTLANDINST 5216.1U
LISTS A, B, C, and D

3-16
TAB F
PROPERTY SPOT CHECK

Facility: _____ DEPT/LPO: _____

ITEM NAME	SERVICE TAG #/BARCODE	ITEM NAME	SERVICE TAG #/BARCODE
LAPTOP:		COMPUTER DESKTOP:	
MONITOR:		REPLICATOR:	
CAC READER:		PRINTER:	
SOFTWARE:		SCANNER:	
TYPEWRITER:		HUB:	
AVERMEDIA:		UPS:	
FAX MACHINE:		FAX MACHINE:	
ZIP DRIVE:		LCD PROJECTOR:	
MISC:		ENGRAVING MACHINE:	

PLEASE ANNOTATE CURRENT DEPARTMENT HEAD NAME AND ALL NRD PROPERTY NUMBERS. CHECK CLOSETS, STOREROOMS, DESK DRAWERS, ETC.

MICROCOMPUTER STANDARD OPERATING PROCEDURES

1. INTRODUCTION

a. The Department of the Navy (DON) Information Assurance (IA) Program, OPNAVINST 5239.1C, requires assurance that security procedures are developed, documented, and presented to all users for all Information Systems (IS). This directive was written to comply with that program.

b. Navy Recruiting Command's microcomputer systems and related assets will be protected in accordance with Standard Operating Procedures (SOP). Security requirements increase in stringency with level of data, mode of operation, type of environment, risk of exposure and costs. The operating procedures in this document will afford adequate protection for all microcomputer and laptop/notebook systems.

c. References made to an Information System Security Officer (ISSO) in the following SOP manual refer to the immediate person at Navy Recruiting District (NRD) who is responsible for Information System (IS) Security.

2. IS SECURITY PLAN COMMAND POLICY. Compliance with applicable IS security regulations is mandatory. Non-compliance with IS security policy and regulations constitutes a security violation/incident. CNRC information systems are accredited to process Sensitive but Unclassified information in the system high security mode of operation. Accordingly, strict adherence to the policies and procedures identified in this SOP is essential. The following are areas that have been included in policy and will be enforced:

a. User Access. User access to information systems and the data they produce shall be strictly limited and based on the user's established need to access such systems and data. Each person who requires access to command information systems and resources must be trained in general computer security procedures and authorized in writing by the command ISSO.

b. Passwords. The password should not be in the dictionary, should not be any variation of one's name, and should not be a birth date. Passwords must be a minimum of eight or maximum of fifteen characters in length, not representing words, names, or phrases, must contain a combination of letters, numbers and special characters such as the "&" sign. Users are not to share passwords nor keep passwords in unsecured location such as on written notes, hard disk storage lists or script files. The host communications will allow three attempts to enter correct identification and password. Following

three failed attempts, the host computer will terminate connection and lock the user out of the system. Passwords must be changed every 90 days.

c. Individual Accountability. CNRC information systems users will be identified by access controls including user passwords and internal software security controls. Access to, and activity within, CNRC's computer systems will be strictly controlled and monitored by the command Information Systems security staff.

(1) Unless access to an external or internal function or system is specifically allowed, the function or system access is not allowed. Allowing only the minimum set of accesses ensures that if users make mistakes, or if intruders succeed in masquerading as legitimate users, the scope of the potential damage is limited.

(2) Violations of this SOP or reference (a) include, but are not limited to, the use of the Internet and/or e-mail for other than official business. Unauthorized purposes and possession of games or other entertainment software on the government workstation is prohibited. Infractions will be charged under the Manual of Courts-Martial, United States, 2012 for military personnel. Remedies for disciplinary action against civilian employees who are in violation could be reprimand, suspension, or removal depending on mitigating or aggravating factors. The appropriate contract delivery order "Standards Enforcement" sections applies for contractor personnel.

d. Monitoring. Only security-appointed personnel (CNRC ISSM, District ISSO, Network Security Officer, and System Administrators (SYSADs) are authorized to monitor ISs. Monitoring will be conducted per NAVSO P-5239.08 and to the extent necessary to ensure that only official government business and other authorized purposes are conducted.

e. Physical Control. Working areas shall be secured during non-working hours. All personnel are responsible for maintaining positive control of visitors in the work space. Unauthorized visitors shall be assisted and escorted.

(1) The District Headquarters is protected by key and cipher lock after hours.

(2) Notebook computers are both expensive and highly pilferable. Extra caution must be taken to ensure that these machines are secured at all times. Systems must not be left in clear

view in unattended vehicles or any where which could result in theft or damage. Each individual assigned a notebook computer must be aware of these possibilities and take extra measures to ensure the safety of the notebook computer.

f. Internet Web Browsing

(1) Internet usage will be for official government business or other authorized purposes only. Users will not access Internet Web sites whose contents might be considered pornographic. Users are prohibited from downloading and/or displaying any material that is considered pornographic or offensive in nature, including all audio and visual material. Users will not access or download from Internet Web sites whose content that may promote racism, bigotry, or anti-semitism. Users will not conduct or promote private business enterprises from government systems.

(2) CNRC provides authorized users with access to unclassified public networks for the sole purpose of communication that is directly related to official unclassified government business and other authorized purposes. Any violation of the following can result in disciplinary or administrative action. The Joint Ethics Regulation, permissible use of the Internet enhances the users' professional skills and thus serves a legitimate public interest. Permissible uses are defined to include all uses not prohibited by law, regulation, instruction or command policy. Permissible uses indicated by the Joint Ethics Regulation generally require supervisor's permission. Prohibited uses include:

(a) Introducing classified information into an unclassified system or environment.

(b) Accessing, storing, processing, displaying, distributing, transmitting, or viewing material that is pornographic, racist, promotive of hate crimes, or subversive in nature.

(c) Storing, accessing, processing or distributing sensitive, "For Official Use Only" or Privacy Act protected information in violation of established security and information policies.

(d) Downloading software for use on any CNRC computers.

(e) Knowingly writing, coding, compiling, storing, transmitting or transferring malicious software code, to include viruses, logic bomb, worms and macro viruses.

(f) Promoting partisan political activity.

(g) Disseminating religious materials outside an established command religious program.

(h) Using the system for personal financial gain, such as advertising or soliciting services or sale of personal property, with the exception of utilizing a command-approved mechanism such as a Welfare and Recreation Electronic Bulletin Board for advertising personal items for sale.

(i) Fund raising activities, either for profit or non-profit unless the activity is specifically approved by the command.

(j) Gambling, wagering or placing of any bets.

(k) Writing, forwarding or participating in chain letters.

(l) Posting personal home pages.

(m) Personal encryption of electronic communications is strictly prohibited.

g. Information System Product Control. Information system memory media, print outs and CRT monitor integrity is the responsibility of everyone authorized to use command information systems or networks. Specifically:

(1) Information system memory media, classified or unclassified, shall not be removed or brought into the command without approval of the command ISSO.

(2) All unlabeled information system media found within the command shall be protected as classified material and forwarded to the Departmental and or command ISSO for final determination.

(3) Monitor (CRT) displays will be protected against casual observation of terminal content.

(4) Operators are required to log out of the system when not in use. Terminal lockout software may be used to disable the terminal when there is a requirement for a user to be away from their system for less than fifteen minutes. After fifteen minutes the user shall log out.

(5) Declassifying, destroying and clearing classified magnetic media, and CRT monitors shall be in accordance with SECNAVINST 5000.2E and SECNAVINST 5510.36A. Information system hard copies (printouts) will be handled and destroyed in accordance with NAVSO P-5239-15.

h. License/Copyright. Adherence to software licensing agreements for copyrighted software packages used within the command will be strictly enforced. The System Administrators will closely monitor prepared software packages to ensure licensing/copyright integrity is maintained.

(1) Copyrighted software will not be copied beyond the specification of the copyright owner. Site licensing agreements will be applied as directed by the contract governing the use of the software. The use of copied or pirated software is prohibited.

(2) Personnel are prohibited from using non-government issued software.

(3) Prior to installation of an IS, all software (i.e., commercial "in-the-shrink" software, public domain freeware/shareware, or software from unofficial sources) shall undergo a formal review or evaluation by the System Administrators to ensure it is free of malicious code. Additionally, each IS will have virus detection software installed to automatically scan the system upon log-on.

(4) Privately owned software is prohibited within command-controlled workspaces. Incidents of such use will be reported immediately to the command ISSO.

(5) Personnel are prohibited from using government-owned equipment for unofficial or private business (e.g., to play games, generate unofficial correspondence, etc.).

(6) Personnel are restricted in the use of privately owned computers and/or software to perform government work. Also, privately owned PCs are prohibited from use in government spaces without written request from the user and written permission from the command ISSO or CNRC ISSM.

i. Information System Security Incidents. All incidents that influence the security and integrity of command computer systems will be reported immediately to the local command ISSO. The local command ISSO will then investigate each incident thoroughly and recommend appropriate corrective action to prevent recurrence to the local commanding officer. The local command ISSO will report all security violations and/or incidents to the CNRC ISSM, utilizing enclosure (4).

3. ORGANIZATION AND RESPONSIBILITIES. The Designated Approving Authority (DAA) for CNRC is the Deputy Commander. The IS Security Manager (ISSM) is the focal point and principal advisor to the DAA for the INCOSEC Program. The District information system security

staff consists of the Information System Security Officer (ISSO), and all Terminal Area Security Officers (TASOs).

a. **Information System Security Officer (ISSO)**. Each NRD will appoint a command ISSO in writing. The command ISSO serves as the focal point on all matters dealing with the security of command information system assets for the IS system(s) and networks in their area of responsibility. In fulfilling this responsibility the command ISSO will:

(1) Enforce command information system security policies as they apply to the specific information systems and networks assigned.

(2) Develop system or network standard operating procedures for information system security safeguards consistent with command information system security policies. As a minimum such plans will contain procedures relevant to:

(a) User access - Users access to command information systems or networks will be strictly limited to those who possess written authorization from the command ISSO, have the proper security clearance and require access to meet their professional responsibilities.

(b) Data integrity - Each file or collection of data in the information system or network will have an identifiable origin and use.

(c) Application software and system software protection, including clearing, declassifying and destroying information system software media.

(d) Classified and unclassified data safeguards and procedures will be consistent with command information system policies and Computer Security Act of 1987 (Public Law 100-235) and DOD Directive 8500.01E.

(e) Identify risks and develop appropriate contingencies and countermeasures to provide for continued operations and safeguard information system assets and resources from alterations, damage, destruction, inadvertent or unauthorized disclosure and misappropriation.

(f) Establish information system configuration controls as they relate to specific security needs of systems hardware, software and peripheral equipment.

(2) Establish and maintain an up-to-date inventory of all information system equipment and licensed or proprietary software.

(3) Develop, manage and control the distribution and security of lists consisting of terminal user access parameters and passwords.

(4) Audit system activity including identification of the levels and types of data processed and monitor activities at user terminal locations to ensure compliance with information system security policies and procedures.

(5) Monitor, test and evaluate any configuration change in information systems that may affect the command information security posture.

(6) Review and monitor procurement submissions for information system equipment and software to ensure compliance with information security regulations.

(7) Submit a written report to the CNRC ISSM on any activities, patterns or circumstances, which may adversely affect command information system security, resources, or mission.

(8) In cooperation with CNRC ISSM, ensure that sanitizing procedures are followed when information system equipment or magnetic storage devices are prepared for release.

(9) Investigate and report all incidents of physical and personal security deficiencies in writing to the CNRC ISSM.

(10) Utilize the IS Security Training Plan contained in reference (a) for local training program. Training may be formal or informal but broad enough in scope to cover both operator and supervisor skill levels.

(11) Identify and recommend system security improvements to the CNRC ISSM and maintain close and continuous coordination with the CNRC ISSM on matters of command information system security interests.

(12) Perform periodic inspection of user terminal locations to ensure adherence to information system security policies and procedures.

(13) Coordinate directly with the CNRC ISSM on all matters concerning command information system security interests.

b. **Terminal Area Security Officer (TASO)**. The TASO is appointed in writing by the Commanding Officer. Within each Navy Recruiting Station shall be one TASO which will normally be the Leading Petty

Officer (LPO). TASOs provide, enforce and maintain day-to-day user and security control over all command IS terminal assets. In meeting this responsibility, each TASO will:

(1) Identify information systems security risks and ensure that all security requirements and countermeasures are implemented for all remote terminal users.

(2) Assist the command ISSO in developing standing operating procedures that identify specific contingency measures, security requirements and operating procedures for each terminal area. Indoctrinate terminal users on applicable security policies and procedures prior to their access into the system or network.

(3) Ensure that each terminal user's identity, need-to-know, level of clearance and access authorization are established commensurate with the data available from that terminal.

(4) Be aware of the identity of each person authorized access to computer terminals within their area of responsibility.

(5) Implement controls to prevent entry of unauthorized transactions through remote terminal devices.

(6) Report all practices dangerous to overall system security and all instances of system security violations to the command ISSO.

(7) Assist the command ISSO in the maintenance of overall information system security.

(8) Maintain central accountability, inventory and positive control over all peripheral and additional equipment and magnetic media.

(9) Ensure current Virus Scanning Software is installed and enabled on all PCs within your area of responsibility.

c. **End-User**. Security related tasks associated with the use of a workstation rests with each end-user. Users will avoid fraud, waste, and abuse of IS resources. The most important user responsibility is the protection of passwords. Additional responsibilities include, but are not limited to the following:

(1) Know who your command ISSO/TASO are and how to contact that individual.

(2) Follow the policies and procedures that have been established for the activity's INFOSEC program.

(3) Support and promote good security practices. For example: Memorize your password, never share your password or allow it to be seen by others and avoid giving another person access to a computer while logged on with your user-id and password.

(4) Mark all media commensurate with the sensitivity of the data stored on that media.

(5) Comply with the command's software copyright policy and never use unapproved software.

(6) Log off your workstation when leaving the computer area for an extended period (more than one hour). Display a password-protected screensaver when leaving the computer area for periods less than an hour.

(7) Do not remove government owned computer resources (hardware, software, data, etc.) from the Command's premises without proper authorization and password control.

(8) Avoid leaving sensitive data displayed in a manner that may compromise the data.

(9) Make backup copies (diskettes) of all critical files and applications stored in the workstation. Store these critical files in a secure location away from the immediate work area.

(10) Follow security incident and violation reporting procedures.

(11) Maintain physical security of your workstation, ensuring that proper security measures are in place to protect the assets. Laptop computers should be placed in an appropriate locked container.

4. **POLICIES**

a. Communications Security/Monitoring and Analysis Policy. The policies, practices and procedures apply to all command personnel employees authorized to use CNRC Information Technology (IT) assets. It is essential that all detected incidents involving malicious activity targeted against or occurring within CNRC information infrastructures be reported and evaluated promptly to ensure data confidentiality, information integrity and service availability is maintained.

b. Electronic Mail (E-Mail Policy)

(1) E-Mail Accounts. CNRC provided e-mail accounts, regardless whether they are accessed from personal or government owned computer systems, must be authorized by the CNRC Information System Department, Network Services Division Officer and the command ISSO. Each account shall be used for conducting official business only. Under no circumstances will individuals engage in discussions or pass classified, Sensitive but Unclassified, For Official Use Only, Privacy Act, or command mission/operation information. Any instance of user misuse of a command computer system may result in immediate termination of e-mail account privileges and possible disciplinary action. CNRC e-mail accounts will be administered by the CNRC Information Systems Department based on mission requirements and available resources and will only be granted to users who have their chain-of-command's recommendation.

(2) Acceptable uses of E-Mail. CNRC provided e-mail is for official use and authorized purposes only.

(a) Official use is any communication determined necessary in the interest of CNRC by the first supervisor in the employee's chain-of-command.

(b) Authorized purposes include:

1. Communications made by CNRC personnel while traveling on government business to receive e-mail for business purposes.

2. Communications with family members to notify them of official business or transportation.

3. Usual workplace communication if it is of such duration and frequency as to not adversely affect the performance of official duties of the District employee, and are, when possible, made during the employee's personal time.

(c) All official e-mail will be sent from a CNRC account. This will allow easier identification of the sender and promotes professionalism. Sensitive unclassified information shall only be sent to authorized recipients via secured or encrypted means.

(d) Only Department Heads and above, or their designees, shall have access to the "All Hands" list for mass mailing.

(3) Unacceptable uses of Electronic Mail

(a) Unauthorized e-mail use is:

1. Any communication that reflects adversely on CNRC, the U.S. Navy, and or the DoD.

2. Excessively burdens CNRC's information systems capabilities.

3. Creates a cost to CNRC in the form of copyright violations and man-hours of staff personnel in fixing/correcting the misuse.

(4) Other prohibited Internet activities include:

(a) Sending large attachments such as graphics, databases, and other large applications with the e-mail messages as they will be returned by the system. The maximum size that can be accommodated for Internet attachments is five Megabytes. Laptops on the road may have a slow connection and lack the capability to receive large files. Files that contain graphics should be posted to the respective organization's bulletin board for disbursement.

(b) Sending chain letters or advertisements of private or social interests (except in the case of the unofficial bulletin board for private sale of personal items). In addition, no jokes or games are to be distributed via the e-mail system. Any such item received should not be forwarded but deleted upon receipt.

(c) The transmission of pornographic or sexually explicit materials or materials containing profane or unprofessional language, questionable humor, or for sexual harassment is strictly prohibited.

(d) Transmitting classified or sensitive information in the clear is prohibited.

(5) CNRC's e-mail system is NOT to be used for unprofessional or derogatory personal remarks that are directed towards an individual or groups of individuals.

(6) Any infractions of the e-mail system will be immediately reported to the CNRC Information Systems Department.

c. Communications

(1) Each employee is responsible for the content of all text, audio and/or images that they place and/or send over CNRC's e-mail system. No email communications may be sent which hide the identity of the sender and/or represents the sender as someone else.

(2) Any message or information sent by an employee of CNRC via the e-mail system are statements that reflect on CNRC. Even if the user includes a personal "disclaimer" in the electronic message, there is still a connection to CNRC, and the statements may be tied to CNRC policy.

(3) All communications sent by District employees via CNRC's e-mail system must comply with this and other CNRC policies and may not disclose classified information.

(4) Command personnel are responsible for ensuring that appropriate labels and statements are applied (i.e., Privacy Act, For Official Use Only, etc.) prior to transmission.

(5) All communications on CNRC's information systems may be monitored.

d. Security

(1) The CNRC Information System Department routinely monitors usage patterns for CNRC's e-mail communications. The reasons for this monitoring are many, including cost analysis/allocation and the management of CNRC's gateway to the Internet.

(2) All messages created, sent, or retrieved over the CNRC provided e-mail system are the property of the U.S. Government and should be considered public information. CNRC, on behalf of the U.S. Government, reserves the right to access and monitor ALL messages and files transmitted via the CNRC provided e-mail system.

(3) Employees should NOT assume electronic communications are totally private and should transmit personal data in other ways.

(4) Copies of e-mail transmissions are subject to possible release under the Freedom of Information Act and discovery in litigation. They are also subject to the records retention requirements of the Federal Records Act.

e. Information System Security Incident Report Policy. A security incident is any attempt to exploit DoN information systems or networks. Security incidents include: Penetration of computer systems, exploitation of technical and administrative vulnerabilities, introduction of computer viruses or other forms of malicious code, and theft or destruction of hardware, software, or data. These types of attacks can result in the compromise of information, denial of service, and other related disruptions that can severely impact the command's mission and function. Users must report all security incidents or perception of an incident to the

command ISSO. The command ISSO will complete and forward enclosure (4), NAVCRUIT 5239/1, AIS Security Incident Report, to the CNRC ISSM. The report may be e-mailed or faxed. The CNRC ISSM will investigate the report and provide recommendation to the CNRC Information Systems Department concerning if the NAVCIRT at the Fleet Information Warfare Center needs to be notified. The CNRC Information Systems Department Director and Designated Approving Authority (DAA) will make the determination if NAVCIRT needs to be notified.

f. Internet Policy

(1) Internet Access. CNRC user accounts, regardless whether they are accessed from personal or government owned computer systems, must be authorized in writing by the CNRC Information Systems Department and the command ISSO. Each account shall be used for conducting official business only. Under no circumstances will individuals engage in discussions or pass classified, sensitive but unclassified, For Official Use Only, Privacy Act, or command mission/operation information. Any instance of user misuse of a command computer system may result in immediate termination of user account privileges and possible disciplinary action.

(2) User Agreement. Enclosure (3), NAVCRUIT 5239/5 CNRC User Responsibility Agreement, shall be prepared and signed by each individual requiring a command Internet access account. This form outlines specific security controls, defines individual responsibilities, and establishes special user restrictions. This User Agreement shall be administered and retained by the command ISSO.

(3) Importing Data. The transfer of software from the Internet to other command computer networks shall be strictly controlled and closely monitored to prevent the introduction of malicious code and the unauthorized use of copyrighted software. Only authorized software as outlined in reference (a) may be introduced into command computer systems. Under no circumstances shall command Internet users access provocative web sites, image files or user groups.

(4) Scanning Policy. All software must be scanned for malicious code using the most current virus scanning software prior to introduction into any other command computer network.

(5) Exporting Data. Special precautions must be taken when transmitting data over networks accessible to the general public. Only unclassified official information may be posted to the general public. Users should not engage in discussions about command missions, functions, activities or personnel.

(6) Information System Security. Anonymity does not exist for persons using command Internet work accounts. Users must understand that they are individually accountable for any actions taken with their accounts and that those actions can and (when system management concerns warrant) are traced back to their origin. Internet users who participate in open discussions with outside users must exercise due cautions when exchanging e-mail or transferring data to ensure neither classified nor sensitive information is inadvertently disclosed.

(7) Suspicious Activities. Command personnel must take special precautions, wherever possible, to authenticate the identity of those persons with whom they are communicating. Personnel must be alert to unusual, undue or unwarranted interest or solicitation for information by unknown persons or organizations. All incidents of intruders, file tampering, service disruptions, probing, suspicious inquires or other questionable activities must be reported.

(8) User Identification and Authentication. All command Internet access accounts will employ strict user identification and authentication countermeasures. Internet user identification shall be by user's real name; aliases are not authorized. Passwords should be at least eight characters in length and may be any combination of upper and lower case letters, numbers and punctuation marks. Users will be required to change their passwords every 90 days. Account management software automatically locks out a user from their account after three unsuccessful login attempts.

(9) Audit. Centralized monitoring and management of command Internet access accounts shall be performed by the CNRC Information Systems Department. Special audit features will be enabled to provide the CNRC IS Director with a comprehensive overview of command Internet host account activities. The Director shall conduct unannounced threat assessments and Internet security sweeps on individual user accounts to identify vulnerabilities; ensure that proper user security controls, countermeasures, and features are employed; protect against improper or unauthorized use; detect malicious activity or network intrusion attempts; and verify appropriate system performance thresholds are maintained.

g. Personally Owned Hardware/Software Policy.

(1) Privately owned PCs and privately owned software are prohibited within command-controlled workspaces. Incidents of such use will be reported.

(2) No personal computer systems are authorized to connect to the physical LAN connection. CNRC has provided for each employee issued with a microcomputer the required software for proper connection to the CNRC LAN/WAN.

(3) Privately owned and or privately purchased software is prohibited from being downloaded on ANY CNRC IS asset.

(4) CNRC/NRD licenses the use of computer software from a variety of companies and does not own this software, unless authorized by the software developer. The command does not have the right to reproduce the software except for backup purposes.

(5) CNRC does not condone the illegal duplication of software. Command members who make, acquire, or use unauthorized copies of computer software shall be disciplined as appropriate under the circumstances.

h. Notebook Computer Policy. Reference (c) outlines policy for notebook computers. Normally, notebook computers cost significantly more than a comparable desktop model. Because of their construction, mobility and diverse environmental exposures, notebook computers must be given special care and consideration. The funds invested in a notebook computer can best be protected by adhering to specific guidelines for the care, handling and security of the system.

(1) SPECIAL CONSIDERATIONS

(a) Temperature. Notebook computers are equipped with liquid crystal displays which are sensitive to temperature extremes. Consequently, notebooks may not be exposed to extreme conditions where temperatures are at or below freezing and then operated immediately. Anytime a notebook is exposed to extreme cold conditions, the system must warm up to room temperature before operation in order to prevent damage. Failure to permit the notebook to warm up to room temperature may cause condensation accumulation which can result in permanent damage to the system. The normal operating temperature range for notebooks is between 40 and 100 degrees Fahrenheit. Additionally, no system should be stored or kept in temperature extremes less than -4 or greater than +140 degrees Fahrenheit. **With respect to this, a dangerous environment includes trunks of cars at any time the outside temperature is below 10 degrees or greater than 75 degrees Fahrenheit.**

(b) Physical Security. Notebook computers are both expensive and highly pilferable. Extra caution must be taken to ensure that these machines are secured at all times. Systems must not be left in clear view in unattended vehicles or anywhere which

could result in theft or damage. Each individual assigned a notebook computer must be aware of these possibilities and take extra measures to ensure the safety of the notebook computer.

(c) Personal Security. Extreme caution must be taken in some areas of the country for the protection of the individual as well as the notebook computer. Personnel with custody of notebook computers should not endanger themselves by carrying the computer when doing so would make them more prone to attack or robbery. Discretion and caution are especially important at night and in high crime areas. If the notebook must be transported during times of increased vulnerability, carrying the computer in a briefcase or gym bag instead of the computer carrying case may reduce the risk of an incident.

(2) ACCOUNTABILITY. Each individual assigned a notebook computer will sign a COMNAVCRUITCOM Custody Card, enclosure (5), acknowledging responsibility for the notebook computer. The individual whose name appears on the custody listing will be held accountable for the computer's care and safety. In the event of loss, theft or damage as a result of possible negligence, appropriate authorities will be notified and an investigation conducted. In all cases of lost, stolen or questionable damage, an Incident Report will be completed and forwarded to CNRC in accordance with reference (a). Any disciplinary action resulting from custodian negligence will be handled by Navy authorities.

i. ENFORCEMENT

(1) The microcomputer user is responsible for reporting any damage, destruction, theft, or unauthorized disclosure of any hardware, software, data, or supporting documents. Reports must be filed immediately via the ISSO. Security incident reporting is an integral part of any IS plan. The IS Security Incident Report will be used in Navy Recruiting.

(2) The ISSO/TASO is responsible for ensuring compliance with the procedures described in this document and for reporting any security violations. Security incident reporting includes the reporting of any hardware, software, or data theft. The ISSO and TASOs are required to report all security incidents. These incidents must be submitted to the ISSO using enclosure (4) of this directive.

(3) Any significant changes in system configuration, i.e., relocation, data classification level, operating mode, etc., may require that security procedures be reevaluated and/or revised and shall be reported to the ISSO.

(4) The ISSO shall review this document annually for accuracy.

MICROCOMPUTER STANDARD OPERATING PROCEDURES (SOPs) REVIEW ACKNOWLEDGEMENT

I acknowledge that I have read, understood, and will adhere to the Microcomputer SOPs of Navy Recruiting District Portland.

I understand that the conditions of my user authorization include:

(a) familiarity with the conditions of information disclosure under the Privacy Act and Freedom of Information Act, as prescribed in SECNAVINST 5211.5E;

(b) use of the system for assigned duties only;

(c) non-disclosure of my password;

(d) adherence to all security policies and procedures as defined in the Microcomputer SOPs;

(e) reporting of any suspected violation of security, including disclosure of information protected by the Privacy Act, to the ISSO/or my supervisor.

SIGNATURE OF USER	DATE	SIGNATURE OF ISSO/TASO

INFORMATION SYSTEM (IS)
SECURITY BRIEFING/USER RESPONSIBILITY AGREEMENT
(PUBLIC-ACCESS NETWORK (INTERNET))

Name_____ Rank/Rate _____ SSN _____

SECURITY BRIEFING

1. Purpose. To emphasize individual responsibilities pertaining to all CNRC IS systems located within the COMNAVCRUITCOM. Also, to outline individual responsibilities and identify specific security controls required for access within any CNRC public-access network, such as the Internet.

2. General. The security of Sensitive Unclassified information is based on the principles of individual responsibility, accountability and need-to-know. IS security, like all other security disciplines, depends upon each individual. The advent of public-access computing environments poses special security risks and threats to the integrity of government data and privacy information. Whether access is achieved from within a command or by personal computer, activities within government sponsored Internet host accounts shall be restricted to unclassified, U.S. Government official business only.

3. Responsibilities. The responsibility for the security of Sensitive Unclassified information used within COMNAVCRUITCOM computer systems rests with each operator. Regardless of countermeasures established to protect the confidentiality, preserve the integrity or ensure the availability of sensitive computer systems, networks or the data processed, they provide little security if ignored by individual users. The following IS User Agreement outlines basic safeguards which must be closely followed when using command computer assets. Official U.S. Government Internet host accounts are established to provide a convenient source to acquire and review state-of-the-art-information; analyze and exchange technical data; preview and evaluate research initiatives; and facilitate information exchange, communications and training. Because of security threats and vulnerabilities inherent within public access computing environments, special countermeasures must be established to preserve the integrity, confidentiality and availability of sensitive data and resources.

USER AGREEMENT (PUBLIC-ACCESS (INTERNET))

I understand...

- The use of CNRC public-access host accounts and computer resources is strictly limited to official government business only.
- Private or personal use of command sponsored Internet services is strictly prohibited.
- I am responsible for controlling the content and determining the sensitivity and integrity of any file I create, modify or retransmit.
- My IS Password(s) are confidential and may not be divulged to anyone, except as may be required by the command ISSO.
- My Internet password is an important countermeasure in maintaining the security and integrity of sensitive government information and resources.
- I may not import any proprietary computer software, unauthorized software, provocative images, or personal data into any command Internet host account without specific approval from the command ISSO.

ENCLOSURE(3)

- I understand that anonymity does not exist on the Internet and that all my activities can ultimately be traced back to this command.
- My Terminal Area Security Officer (TASO) is my primary point-of-contact for any problems or questions concerning IS Security.
- I must immediately report any violation of IS security or any other inappropriate activity I observe or suspect directly to my TASO or the command ISSO.
- Internet host accounts are subject to authorized monitoring and unannounced security sweeps to ensure established security countermeasures are functioning, protect against unauthorized use, and verify the presence and performance of applicable security features.
- Any attempt to circumvent Internet security safeguards or misuse command Internet services will result in immediate termination of my government Internet access and may be referred for administrative or punitive actions.
- If monitoring reveals possible evidence of criminal activity, such evidence may be provided to law enforcement personnel.
- All command computer systems are subject to authorized monitoring to ensure system functionality, verify the application of prescribed security countermeasures, and protect against unauthorized use.
- If monitoring reveals possible evidence of criminal activity, such evidence may be provided to law enforcement personnel.
- By my signature I expressly consent to such monitoring.

I will not...

- Disclose, publish, discuss, or exchange classified, Unclassified Sensitive, privacy or command mission/operation information.
- Circumvent any Internet security countermeasure or safeguard.
- Probe or attempt to break in or gain access to any system on the Internet to which I am not authorized access.

I will...

- Exercise good judgment, personal discretion and professional integrity when accessing the Internet.
- Establish, protect, and maintain my password as directed by the command ISSO.
- Use command Internet host accounts for only official U.S. Government business.
- Report any suspicious or unusual activity occurring within or targeted against our command Internet systems directly to the command ISSO.
- Submit professional papers, articles, technical reports, personal resumes, and any other published works I intend to distribute via the Internet to the Command Security Manager for prepublication review. *NOTE: Prepublication review does not apply to "E-mail" messages.*
- Properly log off my account upon completion of work or prior to departing the work area.
- Report any weakness in Internet security countermeasures or procedures I observe or encounter to the command ISSO.
- By signing below I understand that my command Internet host account is subject to authorized monitoring and security sweeps, and that any evidence of illegal activities will be reported to law enforcement personnel.

ACCOUNT PRIVILEGES

Account Permissions Group: _____
(OTHER/STAFF/WEBADM/SYSADM/WHEEL)

Type of Remote Access Authorized: _____
(NONE/TTY/SLIP/PPP)

_____ _____
Rank/Rate, Name (Last, First, M.I.) SSN

_____ _____
Service Signature Date

INTERNET USER AUTHORIZATION

In consideration of your acknowledged understanding of basic IS security practices and procedures; your verified security clearance and established "need-to-know", you are hereby authorized limited access to operate and use command IS computer systems and resources necessary to fulfill your individual responsibilities; also your understanding of the command's Internet security policy, practices, and procedures; have hereby authorized you access to a command Internet host account, and command Internet equipment resources to fulfill your professional responsibilities.

Your access entitles you to use the Internet via a U.S. Government host account to fulfill your professional duties only. Attempts to probe or break-in to private accounts; circumvent Internet security controls or countermeasures; disable audit mechanisms or firewalls; or use the command Internet host account for purposes other than which it is intended, may result in suspension of all privileges, or the use of command IS systems and assets for purposes other than which they were intended or accredited, will be considered to be and reported as security violations.

All command computer systems are to be used for official government business by authorized users only. Individual user activities on command computer systems are subject to authorized monitoring without notice by system management or IS security personnel. Anyone using the command's computer systems, expressly consent to such monitoring and is aware that if monitoring reveals evidence of user misfeasance, he/she will be subject to appropriate disciplinary action. The command Internet host account is to be used for official government business only. Personal or private use is prohibited. Individual user activities on command Internet host accounts are subject to authorized monitoring and unannounced security sweeps.

_____
COMMAND ISSO

PRIVACY ACT STATEMENT. Authority to request this information is contained in 5 U.S.C Statute 301 for the purpose of requesting information to ensure that all Navy Recruiting Command military, GS civilian and contractor personnel who have signed this security briefing/user agreement form are correctly identified. Also 10 U.S.C Part II and 14 U.S.C Chapter 11 provide authority for the Command Information System Security Manager to use the above data to ensure proper security indoctrination of all assigned personnel.

AIS SECURITY INCIDENT REPORT

1. From: ISSO,	2. To: NAVCRUITCOM Information Assurance Manager	
3. Via:	4. Report Date:	5. Incident Date:

6. Type of Incident:

- ☐ Waste Fraud Abuse
- ☐ Theft
- ☐ Destruction
- ☐ Modification
- ☐ Other
- ☐ Unauthorized Disclosure
- ☐ Unauthorized User ID
- ☐ Password Violation
- ☐ System Security Related
- ☐ Failure (Specify)

7. Individuals Involved (Name, Rank, Code):

8. Cost of Incident (Downtime, Cost, Etc.):

9. Summary of Incident and Investigation Results:

10. Department Head Recommendation/Comments:

11. Investigating Officer if other than ISSO (Name, Rank):

12. Local Action to Prevent Reoccurrences:

13. Recommended Action by ISSO:

ENCLOSURE(4)

COMNAVCRUITCOM CUSTODY CARD FOR NOTEBOOK COMPUTERS

1. NAVCRUITDIST:	2. NAVCRUITSTA:
3. RECRUITER'S NAME:	4. SOCIAL SECURITY NUMBER: (**LAS-T FOUR DIGITS ONLY**)

5. ACCEPTANCE OF CUSTODY:

I, _____, accept custody of the Notebook Computer
(*Name*)

_____ assigned to me. I am thoroughly
(*Serial Number*)

familiar with the provisions of COMNAVCRUITCOMINST 4400.1 (LSM), Paragraph 305.5.d. I understand that by accepting custody, I will be held accountable for the care and safety of the Notebook Computer assigned to me.

PRIVACY ACT NOTIFICATION

This document contains information covered under the Privacy Act of 1974, 5 USC 552a and its various implementing regulations and must be protected in accordance with those provisions. You, the recipient/user, are obliged to maintain it in a safe, secure and confidential manner. Re-disclosure without consent or as permitted by law is prohibited. Unauthorized re-disclosure or failure to maintain confidentiality subjects you to application of appropriate sanctions. If you have received this correspondence in error, please notify the sender immediately and destroy any copies you have made.

6.	7.
(*Signature of Recruiter*)	(*Date*)

NAVCRUIT 5230/6 (Rev. 3-08)

FOR OFFICIAL USE ONLY WHEN FILLED IN

ENCLOSURE(6)

NAVCRUITDISTPORTLANDINST 5239.1D
26 Mar 13